Congressional Responses

1. Please provide the name and official title of the individual currently fulfilling the responsibilities and duties of agency Chief Information Officer as delineated in the Clinger-Cohen Act 1996 (P.L. 104-106) and the Federal Information Security Management Act of 2002 ('FISMA') (P.L. 107-347). If the individual is serving in an "acting" capacity, please explain the steps you are taking to finalize an appointment to this position.

   Darren B. Ash
   Deputy Executive Director for Information Services and Chief Information Officer (CIO)
   Office of the Executive Director for Operations

2. Since FISMA was enacted in December 2002, how many individuals have served in the agency CIO position and what were the periods of their service?

   There have been a total of four individuals who have served in the agency CIO position. Their names and periods of service are as follows:

   Stuart Reiter - CIO (June 2001 - April 2003)
   Jacqueline Silber - Acting CIO (April 2003 - June 2003)
   Ellis Merschoff - CIO (June 2003 - June 2004)
   Jacqueline Silber - CIO (May 2004 - January 2005)
   Jacqueline Silber - Deputy Executive Director for Information Services and Administration and CIO (February 2005 - May 2007)
   Darren Ash - Deputy Executive Director for Information Services and CIO (May 2007 to present)

3. Does the agency CIO have a direct report relationship to you?

   No.

   If not, to whom does the agency CIO directly report on a day-to-day basis?

   The CIO reports directly to the Executive Director for Operations (EDO), who is the most senior career service executive at the NRC and is responsible for day-to-day agency operations.

4. What functions does the agency CIO's office perform? What is the CIO's jurisdiction within the agency? Also, please describe the structure of the agency CIO's office including total number of employees, their titles, and responsibilities.

   The CIO also serves as the Deputy Executive Director for Information Services. His responsibilities include providing policy direction, leadership and oversight for information technology and information management (IT/IM) activities at the Nuclear Regulatory Commission (NRC). The CIO office is responsible for information technology (IT) infrastructure, applications development, business process improvement, and information management services. The CIO represents the NRC on the Federal CIO Council and is designated as the NRC Chief Freedom of Information

Act Officer. The CIO provides leadership, guidance and direction to the Office of Information Services (OIS).

OIS has 176 FTE. The functions for OIS are located at: http://www.nrc.gov/about-nrc/organization/oisfuncdesc.html. This information, including the organizational structure is also attached.

5. Is the agency CIO a member of formal executive-level strategic planning, budget, and program-area process re-design committees, groups, or councils established in?

Yes. The CIO is a member of the NRC's Program Review Committee (PRC), is the Chair of the Information Technology Senior Advisory Council (ITSAC), and a member of the Executive Director for Operations Executive Team.

a. What are the responsibilities of the agency CIO on these committees and groups?

PRC - The PRC is an executive management review body to facilitate decision making regarding the NRC's long range program planning, budgeting, and performance management. The CIO brings an IT/IM perspective to the executive management review.

ITSAC - Established by the CIO, it is a cross-agency senior management investment review committee established to make agency-level recommendations on funding and management of the NRC's IT capital investment portfolio. The ITSAC is chaired by the CIO and its members consist of Office Directors from major NRC offices and a rotating Regional Administrator. The ITSAC serves as a forum for addressing agency-level IT initiatives and issues.

EDO Executive Team - Comprised of the three Deputy Executive Directors, they assist the EDO in the overall planning, management, control, and coordination of the operational and administrative activities of the agency. This includes directing policy development, agency operational activities, and implementation of Commission policy directives.

b. Has the agency CIO made, or played a vital role in making strategic business decisions for the department/agency? Please provide several noteworthy examples.

Yes. A few noteworthy examples are:

Infrastructure and Services Support Contract (ISSC) - The CIO championed the successful implementation and ongoing operation of the agencywide infrastructure services support program, which uses a hybrid approach of providing desktop services (desktop installation, maintenance and customer support services, equipment refresh, and LAN/WAN connectivity) at specific levels of performance based on the number of users (seats), and provides technical services such as infrastructure development on a level of effort basis. Under this approach, the contractor is fully responsible for providing integrated seat services at a fixed price per desktop, including operations and support

for desktop equipment, a help desk function, local and wide area network connectivity, maintenance, and a periodic refresh of equipment, while providing NRC the flexibility needed to support evolving business requirements.

Agencywide Documents Access and Management System (ADAMS) - The NRC received the 2003 Archivist's Achievement Award in Records Management on May 13, 2003, at the National Archives and Records Administration's (NARA) annual Records Administration Conference. The award is in recognition of NRC's work on the development and implementation of ADAMS as an electronic records management system. ADAMS is the first enterprise-wide electronic records management system to receive NARA approval. As a result, OIS has been deeply involved in sharing lessons learned with other agencies who are currently exploring the development and deployment of electronic records management systems. OIS has demonstrated and presented ADAMS to several Federal agencies and at Federal and industry conferences and symposia. OIS continues to work very closely with NARA as it develops policies and procedures governing the development and implementation of electronic records management systems and the transfer of electronic records to NARA for permanent storage.

The IT/IM Strategic Plan - The CIO established an agency-level IT/IM Strategic Planning Group (ISPG) to produce the FY 2008 - 2012 IT/IM Strategic Plan. The IT/IM plan responds to the Federal requirement in the Paperwork Reduction Act and the Clinger-Cohen Act which directs agencies to establish goals and measures of the contribution of IT/IM activities to agency productivity, efficiency, effectiveness and service to the public. The plan describes how IT/IM activities at the NRC help accomplish the agency's mission. The goals, strategies and measures in the plan provide the foundation for directing and assessing the performance of the NRC's IT/IM program through FY 2012. The CIO directly oversees a significant portion of the agency's IT/IM program, but the scope extends to every NRC organization.

6. Please outline the policy, operational, and budget authorities delegated to the CIO. What, if any, additional duties or responsibilities does the agency CIO have other than information resources management?

*As delegated by the EDO, the CIO develops and implements an agencywide framework that includes policies, processes, and procedures for IT capital investments, Enterprise Architecture, information management, and IT security that meets the requirements of Federal statutes and regulations, and guidance from the Office of Management and Budget (*as stated in OMB Circular A-11, Part 7, and Circular A-130) *and the Government Accountability Office.*

The CIO establishes the Project Management Methodology and oversees the management of IT investments. He established the Enterprise Architecture Review Board and approved its charter. He also establishes other review or advisory bodies, as necessary, to involve agency program officials in IT investment planning and management oversight in order to ensure agencywide coordination of IT programs.

The CIO chairs the ITSAC, approves its membership, and approves revisions to its charter as needed. He established the Information Technology Business Council (ITBC)

and approves its membership and charter. The ITSAC sets the IT investment strategy for the agency, assuring a balance of programmatic and infrastructure IT support; reviews, concurs, and prioritizes the IT investment portfolio provided by the ITBC and submits it to the CIO; and, when requested by the CIO, serves as the executive review function for significant issues in the management control and evaluation phases of capital planning and investment control.

7. Do the component organizations that comprise your agency have designated CIOs? If so, please list the component organization, and the name and official title of the person serving as CIO for that component.

   N/A

8. Please tell us (a) how are the component organization CIOs are selected, (b) to whom do they report, and (c) the parameters of the decisional and budgetary authority of the component organizations?

   N/A

9. What percentage of total information management and technology expenditures are controlled or approved by the agency CIO?

   The CIO controls 66 percent of IT/IM expenditures for FY 2007.

   What percentage is controlled by component organizations that comprise your agency?

   The percentage controlled by component organizations within the NRC is 34 percent.

10. What resources does your Department or Agency provide to the CIO office and its organizational components to maintain an effective agencywide security program?

    OIS is responsible for developing and maintaining the agencywide IT security program and for developing policy for the handling of all sensitive unclassified non-safeguards information, including personally identifiable information. OIS develops and maintain risk-based IT security policies, procedures, System Development Life Cycle Management Methodology, and control techniques that cost-effectively reduce IT risks to an acceptable level and ensure that IT security is addressed throughout the life cycle of each NRC information system. OIS provides 8 FTE to support these efforts.

    In addition to the OIS staff noted above, the CIO works with the Office of Nuclear Security Incident Response (NSIR) and the Office of Administration (ADM) to maintain an agencywide information security program. NSIR plans, coordinates, and manages the information security program to protect classified and safeguards information for the agency; administers secure telecommunications, declassification, foreign disclosure of information, foreign ownership, control or influence, and authorized classifiers and safeguards information designators programs; acts as the NRC Central Office of Record for communications security material; operates the NRC's secure communications center; and maintains the certification of NRC's Sensitive Compartmented Information Facility. NSIR provides 7 FTE to support the agencywide information security program.

ADM is responsible for the NRC personnel and physical security programs to establish physical security safeguards for the protection of Headquarters, regional offices, and contractor facilities; assure the safe storage of classified and sensitive unclassified information; and conduct background checks for employees and contractors. ADM provides 9 FTE in support of the agencywide information security program.

11. Please describe the agency CIO's role in developing information technology budget submissions and business case justifications for major information technology investments. Are the CIOs of agency's component organizations involved in these processes? If so, please describe their contributions.

The sponsoring office of an IT investment is responsible for the business justification for the investment. The CIO concurs with IT investments and recommends approval to the EDO or Commission, as appropriate. The CIO reviews programs taking into consideration agency resource requirements; compliance with government-wide guidance/directives; and impact on the agency's architecture, infrastructure, and IT portfolio.

12. Please provide the name and job title of the individual managing privacy issues in the agency? To whom does this individual report and what responsibilities does the individual have?

On March 18, 2005, Mr. Edward T. Baker, III, was designated to serve as the NRC's Senior Agency Official for Privacy, in response to OMB memorandum (M-05-08) dated February 11, 2005. Mr. Baker reports to Darren B. Ash, NRC's CIO. Mr. Baker's full title is Director, OIS and Deputy CIO. His responsibilities include providing principal advice and assistance to the Chairman, the Commissioners, the EDO, Deputy Executive Director for Information Services, and other agency executives to ensure that agency IT/IM resources are selected and managed in a manner that maximizes their value to accomplish the agency's mission and manage risks. For specific questions regarding privacy issues, Russell Nichols is the NRC Freedom of Information Act and Privacy Act Officer.

13. Ensuring adequate information security in the federal government requires skilled and dedicated IT employees. The federal government, for example, finds itself competing against the private sector for talented IT workers. Do federal agencies have the resources necessary to execute the elaborate security measures that are necessary in order to maintain their systems and to keep the government connected to people and businesses?

The IT security skills necessary to maintain secure systems are difficult to find and retain within the Federal government. These skills are in short supply and high demand, requiring higher salaries. A high turnover rate is experienced as individuals with these skills seek more appealing opportunities. This experience is not unique to the NRC. In addition, the NRC's security clearance process for contractors has exacerbated the skill gaps, as major concerns have been identified during the clearance review that require adjudication and/or denial of access. Consequently, there continues to be a challenge maintaining a full and knowledgeable IT security staff. Furthermore, with more frequent and sophisticated attacks of IT systems and infrastructure, it may be advantageous to

move away from measuring adequate information security in the Federal government through a score card approach based on security compliance, and move toward a risk-based approach based on the degree to which systems are secure by the incorporation of mitigating controls and/or the management of risks.

14. What percentage of the total agency budget is allocated for IT?

Of the agency's total FY 2007 budget, 14.5 percent is allocated for IT.

For security?

A total of approximately 1.2 percent of the agency's FY 2007 budget is allocated for information security.

Please provide a breakdown of the IT security budget.

A breakdown of the FY 2007 IT security budget is as follows:

Mission Critical Systems: 46%
IT Infrastructure Systems: 53%
Enterprise Architecture and Planning: 1%